UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/389,842	09/02/1999	EARL LEVINE	P-2100	5948

22801 7590 05/03/2006

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 05/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/389,842	LEVINE ET AL.	
	Examiner	Art Unit	
	Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02/21/2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) *1-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to request for continued examination, and amendment filed on February 21, 2006. Original application contained Claims 1-43. Applicant previously added Claims 44-49, and previously amended Claims 3, 6, 16, 25, and 20. Applicant currently amended Claim Claims 1, 4, 7, 12, 14, 20, 25, 27, 33, 38, 40, 44 and 47. The amendment filed have been entered and made of record. Presently pending claims are 1- 49.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on February 21, 2006 has been entered.

Response to Arguments

Applicant's arguments with respect to claims 1, 7, 12, 14, 20, 25, 27, 33, 38, and 40 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 27-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Moskowitz et al. U. S. Patent No. 6,522,767 ('Moskowitz' hereinafter), and further in view of Iwamura (U. S. Patent 6,425,081).

3. With respect to claim 1, Moskowitz teach a method for tracking a requested signal (see abstract), the method comprising: receiving at a server computer, a request for the requested signal, generating at a server computer transaction identification data which identifies the received request, and including a pattern in the requested signal to form a watermarked signal using a predetermined basis signal, wherein the transaction identification data can be derived from the pattern; further wherein the inclusion of the basis signal in the requested signal is designed to introduce no more than a predetermined maximum level of perceptibility to the requested signal (see abstract; col. 2, lines 26-46; col. 3, lines 19-23).

Although the system disclosed by Moskowitz shows all the features of the claimed limitation, but Moskowitz does not specifically disclose a server side computer causing the

computer to enable tracking the requested signal, and sending watermark signal in response to the request.

In an analogous art, Iwamura, on the other hand discloses computing environment that relates to method and apparatus for providing an electronic watermarking method whereby the illegal activities and the illegal distribution of the original data by a server and a user can be prevented, and to provide an electronic information distribution system therefor. Where he signature generator 22 of the user terminal 20 generates signature information S using its own secret key. The electronic watermark-embedding unit 23 embeds the signature information S, generated by the signature generator 22, in the primary encrypted image data that are transmitted (distributed) by the server terminal 10 (col. 32 line 46 to col.34 line 22). Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Moskowitz and Iwamura, because Iwamura's method of embedding of monitored data by using image data (i.e. watermark) would not only promote security structure in the system of Moskowitz during receiving data from host computing devices but will also provide identifying data that can be securely and robustly included in a digitized signal in a particular efficient manner such that a server computer system can add such data for each delivery of the digitized signal (Iwamura, abstract, and col.1 line 55 to line 64).

4. With respect to claim 7, Moskowitz disclose a method for enabling embedding of transaction-specific identification data into a requested signal, the method comprising: logically dividing the requested signal into segments at a server computer (see col. 4, lines 6-17); for each

segment, embedding a first logical value in the segment to form a first embedded segment (see col. 4, lines 6-17); embedding a second logical value in the segment to form a second embedded segment (see col. 4, lines 6-17); and including both the first and second embedded segments in a composite signal (col. 4, lines 6-17).

Although the system disclosed by Moskowitz shows all the features of the claimed limitation, but Moskowitz does not specifically disclose a server side computer causing the computer to enable tracking the requested signal, and sending watermark signal in response to the request.

In an analogous art, Iwamura, on the other hand discloses computing environment that relates to method and apparatus for providing an electronic watermarking method whereby the illegal activities and the illegal distribution of the original data by a server and a user can be prevented, and to provide an electronic information distribution system therefor. Where he signature generator 22 of the user terminal 20 generates signature information S using its own secret key. The electronic watermark-embedding unit 23 embeds the signature information S, generated by the signature generator 22, in the primary encrypted image data that are transmitted (distributed) by the server terminal 10 (col. 32 line 46 to col.34 line 22). Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Moskowitz and Iwamura, because Iwamura's method of embedding of monitored data by using image data (i.e. watermark) would not only promote security structure in the system of Moskowitz during receiving data from host computing devices but will also provide identifying data that can be securely and robustly included in a digitized signal in a

particular efficient manner such that a server computer system can add such data for each delivery of the digitized signal (Iwamura, abstract, and col.1 line 55 to line 64).

5. With respect to claim 12, Moskowitz disclose a method for embedding transaction-specific identification data into a requested signal (see col. 16, lines 39-45; col. 19, lines 57-61), the method comprising: retrieving at a server computer, a composite signal which includes, for each of one or more corresponding portions of the requested signal, a first marked segment which represents a first logical value embedded in the corresponding portion of the requested signal and a second marked segment which represents a second logical value embedded in the corresponding portion of the requested signal (see col. 1, lines 60-64; col. 2, lines 58-67 to col. 3, lines 19-23); for each of the corresponding portions of the requested signal, selecting segments of the composite signal according to logical values of corresponding bits of the transaction-specific identification data (see col. 1, lines 60-64; col. 2, lines 58-67 to col. 3, lines 19-23); and combining at the server computer the selected segments to form a watermarked signal which includes the transaction-specific identification data embedded therein (see col. 12, lines 6-17; col. 17, lines 18-44).

Although the system disclosed by Moskowitz shows all the features of the claimed limitation, but Moskowitz does not specifically disclose a server side computer causing the computer to enable tracking the requested signal, and sending watermark signal in response to the request.

In an analogous art, Iwamura, on the other hand discloses computing environment that relates to method and apparatus for providing an electronic watermarking method whereby the

illegal activities and the illegal distribution of the original data by a server and a user can be prevented, and to provide an electronic information distribution system therefor. Where he signature generator 22 of the user terminal 20 generates signature information S using its own secret key. The electronic watermark-embedding unit 23 embeds the signature information S, generated by the signature generator 22, in the primary encrypted image data that are transmitted (distributed) by the server terminal 10 (col. 32 line 46 to col.34 line 22). Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Moskowitz and Iwamura, because Iwamura's method of embedding of monitored data by using image data (i.e. watermark) would not only promote security structure in the system of Moskowitz during receiving data from host computing devices but will also provide identifying data that can be securely and robustly included in a digitized signal in a particular efficient manner such that a server computer system can add such data for each delivery of the digitized signal (Iwamura, abstract, and col.1 line 55 to line 64).

6. With respect to claim 14, Moskowitz disclose a computer-readable storage medium on which is stored computer code which, when executed by at a server-side computer, causes the computer to enable tracking a requested signal by: receiving a request for the requested signal, generating transaction identification data which identifies the received request, including a pattern in the requested signal to form a watermarked signal using a predetermined basis signal, wherein the transaction identification data can be derived from the pattern; further wherein the inclusion of the basis signal in the requested signal is designed to introduce no more than a

predetermined maximum level of perceptibility to the requested signal (col. 2, lines 26-46; col. 3,lines 19-23; col. 6,lines 42-52).

Although the system disclosed by Moskowitz shows all the features of the claimed limitation, but Moskowitz does not specifically disclose a server side computer causing the computer to enable tracking the requested signal, and sending watermark signal in response to the request.

In an analogous art, Iwamura, on the other hand discloses computing environment that relates to method and apparatus for providing an electronic watermarking method whereby the illegal activities and the illegal distribution of the original data by a server and a user can be prevented, and to provide an electronic information distribution system therefor. Where he signature generator 22 of the user terminal 20 generates signature information S using its own secret key. The electronic watermark-embedding unit 23 embeds the signature information S, generated by the signature generator 22, in the primary encrypted image data that are transmitted (distributed) by the server terminal 10 (col. 32 line 46 to col.34 line 22). Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Moskowitz and Iwamura, because Iwamura's method of embedding of monitored data by using image data (i.e. watermark) would not only promote security structure in the system of Moskowitz during receiving data from host computing devices but will also provide identifying data that can be securely and robustly included in a digitized signal in a particular efficient manner such that a server computer system can add such data for each delivery of the digitized signal (Iwamura, abstract, and col.1 line 55 to line 64).

7. With respect to claim 20, Moskowitz disclose a computer-readable storage medium on which is stored computer code which, when executed by a server-side computer, causes the computer to enable embedding of transaction-specific identification data into a requested signal by: logically dividing the requested signal into segments, for each segment, embedding a first logical value in the segment to form a first embedded segment, embedding a second logical value in the segment to form a second embedded segment and including both the first and second embedded segments in a composite signal (col. 3, lines 59-67, col. 4, lines 6-17).

Although the system disclosed by Moskowitz shows all the features of the claimed limitation, but Moskowitz does not specifically disclose a server side computer causing the computer to enable tracking the requested signal, and sending watermark signal in response to the request.

In an analogous art, Iwamura, on the other hand discloses computing environment that relates to method and apparatus for providing an electronic watermarking method whereby the illegal activities and the illegal distribution of the original data by a server and a user can be prevented, and to provide an electronic information distribution system therefor. Where he signature generator 22 of the user terminal 20 generates signature information S using its own secret key. The electronic watermark-embedding unit 23 embeds the signature information S, generated by the signature generator 22, in the primary encrypted image data that are transmitted (distributed) by the server terminal 10 (col. 32 line 46 to col.34 line 22). Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Moskowitz and Iwamura, because Iwamura's method of embedding of monitored data by using image data (i.e. watermark) would not only promote security

structure in the system of Moskowitz during receiving data from host computing devices but will also provide identifying data that can be securely and robustly included in a digitized signal in a particular efficient manner such that a server computer system can add such data for each delivery of the digitized signal (Iwamura, abstract, and col.1 line 55 to line 64).

8. With respect to claim 25, Moskowitz disclose a computer-readable storage medium on which is stored computer code which, when executed by server-side computer, causes the computer to enable embedding transaction-specific identification data into a requested signal by: retrieving a composite signal which includes, for each of one or more corresponding portions of the requested signal, a first marked segment which represents a first logical value embedded in the corresponding portion of the requested signal and a second marked segment which represents a second logical value embedded in the corresponding portion of the requested signal (see col. 1, lines 60-64; col. 2, lines 58-67; col. 3, lines 19-23; col. 4, lines 6-17); for each of the corresponding portions of the requested signal, selecting segments of the composite signal according to logical values of corresponding bits of the transaction-specific identification data (see col. 1, lines 60-64; col. 2, lines 58-67; col. 3, lines 19-23; col. 4, lines 6-17); and combining the selected segments to form a watermarked signal which includes the transaction-specific identification data embedded therein (see col. 4, lines 6-17; col. 17, lines 18-44).

Although the system disclosed by Moskowitz shows all the features of the claimed limitation, but Moskowitz does not specifically disclose a server side computer causing the computer to enable tracking the requested signal, and sending watermark signal in response to the request.

In an analogous art, Iwamura, on the other hand discloses computing environment that relates to method and apparatus for providing an electronic watermarking method whereby the illegal activities and the illegal distribution of the original data by a server and a user can be prevented, and to provide an electronic information distribution system therefor. Where he signature generator 22 of the user terminal 20 generates signature information S using its own secret key. The electronic watermark-embedding unit 23 embeds the signature information S, generated by the signature generator 22, in the primary encrypted image data that are transmitted (distributed) by the server terminal 10 (col. 32 line 46 to col.34 line 22). Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Moskowitz and Iwamura, because Iwamura's method of embedding of monitored data by using image data (i.e. watermark) would not only promote security structure in the system of Moskowitz during receiving data from host computing devices but will also provide identifying data that can be securely and robustly included in a digitized signal in a particular efficient manner such that a server computer system can add such data for each delivery of the digitized signal (Iwamura, abstract, and col.1 line 55 to line 64).

9. With respect to claim 27, Moskowitz disclose a server computer system comprising: a processor, a memory coupled to the processor (see col. 11, lines 21-27), and a watermarker which executes in the processor from the memory and which, when executed, enables tracking of a requested signal by: receiving a request for the requested signal, generating transaction identification data which identifies the received request (see col. 10, lines 62-67 to col. 11, lines 21 -27); and including a pattern in the requested signal to form a watermarked signal using a

predetermined basis signal, wherein the transaction identification data can be derived from the pattern; further wherein the inclusion of the basis signal in the requested signal is designed to introduce no more than a predetermined maximum level of perceptibility to the requested signal (see col. 2, lines 26-46; col. 3, lines 19-23).

Although the system disclosed by Moskowitz shows all the features of the claimed limitation, but Moskowitz does not specifically disclose a server side computer causing the computer to enable tracking the requested signal, and sending watermark signal in response to the request.

In an analogous art, Iwamura, on the other hand discloses computing environment that relates to method and apparatus for providing an electronic watermarking method whereby the illegal activities and the illegal distribution of the original data by a server and a user can be prevented, and to provide an electronic information distribution system therefor. Where he signature generator 22 of the user terminal 20 generates signature information S using its own secret key. The electronic watermark-embedding unit 23 embeds the signature information S, generated by the signature generator 22, in the primary encrypted image data that are transmitted (distributed) by the server terminal 10 (col. 32 line 46 to col.34 line 22). Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Moskowitz and Iwamura, because Iwamura's method of embedding of monitored data by using image data (i.e. watermark) would not only promote security structure in the system of Moskowitz during receiving data from host computing devices but will also provide identifying data that can be securely and robustly included in a digitized signal in a

particular efficient manner such that a server computer system can add such data for each delivery of the digitized signal (Iwamura, abstract, and col.1 line 55 to line 64).

10. With respect to claim 33, Moskowitz disclose a server computer system comprising: a processor, a memory coupled to the processor, and a blank watermarker which executes in the processor from the memory and which, when executed, enables embedding of transaction -specific identification data into a requested signal by (see col. 10, lines 62-67; col. 11, lines 1-27): logically dividing the requested signal into segments, for each segment, embedding a first logical value in the segment to form a first embedded segment (see col. 4, lines 6-17); embedding a second logical value in the segment to form a second embedded segment (see col. 4, lines 6-17); and including both the first and second embedded segments in a composite signal (see col. 4, lines 6-17).

Although the system disclosed by Moskowitz shows all the features of the claimed limitation, but Moskowitz does not specifically disclose a server side computer causing the computer to enable tracking the requested signal, and sending watermark signal in response to the request.

In an analogous art, Iwamura, on the other hand discloses computing environment that relates to method and apparatus for providing an electronic watermarking method whereby the illegal activities and the illegal distribution of the original data by a server and a user can be prevented, and to provide an electronic information distribution system therefor. Where he signature generator 22 of the user terminal 20 generates signature information S using its own secret key. The electronic watermark-embedding unit 23 embeds the signature information S,

generated by the signature generator 22, in the primary encrypted image data that are transmitted (distributed) by the server terminal 10 (col. 32 line 46 to col.34 line 22). Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Moskowitz and Iwamura, because Iwamura's method of embedding of monitored data by using image data (i.e. watermark) would not only promote security structure in the system of Moskowitz during receiving data from host computing devices but will also provide identifying data that can be securely and robustly included in a digitized signal in a particular efficient manner such that a server computer system can add such data for each delivery of the digitized signal (Iwamura, abstract, and col.1 line 55 to line 64).

11. With respect to claim 38, Moskowitz disclose a server computer system comprising: a processor, a memory coupled to the processor, and a watermarker which executes in the processor from the memory and which, when executed, embeds transaction-specific identification data into a requested signal (see col. 10, lines 62-67; col. 11, lines 1-27) by: retrieving a composite signal which includes, for each of one or more corresponding portions of the requested signal, a first marked segment which represents a first logical value embedded in the corresponding portion of the requested signal and a second marked segment which represents a second logical value embedded in the corresponding portion of the requested signal (see col. 1, lines 60-64; col. 2, lines 58-67; col. 3, lines 19-23; col. 4, lines 6-17); for each of the corresponding portions of the requested signal, selecting segments of the composite signal according to logical values of corresponding bits of the transaction-specific identification data (see col. col. 1, lines 60-64; col. 2, lines 5867; col. 3, lines 19-23; col. 4, lines 6-17); and

combining the selected segments to form a, watermarked signal which includes the transaction-specific identification data embedded therein (see col.4, lines 6-17; col. 17, lines 18-44).

Although the system disclosed by Moskowitz shows all the features of the claimed limitation, but Moskowitz does not specifically disclose a server side computer causing the computer to enable tracking the requested signal, and sending watermark signal in response to the request.

In an analogous art, Iwamura, on the other hand discloses computing environment that relates to method and apparatus for providing an electronic watermarking method whereby the illegal activities and the illegal distribution of the original data by a server and a user can be prevented, and to provide an electronic information distribution system therefor. Where he signature generator 22 of the user terminal 20 generates signature information S using its own secret key. The electronic watermark-embedding unit 23 embeds the signature information S, generated by the signature generator 22, in the primary encrypted image data that are transmitted (distributed) by the server terminal 10 (col. 32 line 46 to col.34 line 22). Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Moskowitz and Iwamura, because Iwamura's method of embedding of monitored data by using image data (i.e. watermark) would not only promote security structure in the system of Moskowitz during receiving data from host computing devices but will also provide identifying data that can be securely and robustly included in a digitized signal in a particular efficient manner such that a server computer system can add such data for each delivery of the digitized signal (Iwamura, abstract, and col.1 line 55 to line 64).

12. With respect to claim 40, Moskowitz disclose a computer-readable storage medium executable on a server computer on which is stored a signal which comprises: one or more segments of a subject signal (see col. 3, lines 50-59); for each of the segments, a first segment instance representing a first logical value of portion of a pattern which is embedded in the segment, and a second segment instance representing a second logical value of the portion embedded in the segment (see col. 3, lines 59-67 to col. 4, lines 1-17).

Although the system disclosed by Moskowitz shows all the features of the claimed limitation, but Moskowitz does not specifically disclose a server side computer causing the computer to enable tracking the requested signal, and sending watermark signal in response to the request.

In an analogous art, Iwamura, on the other hand discloses computing environment that relates to method and apparatus for providing an electronic watermarking method whereby the illegal activities and the illegal distribution of the original data by a server and a user can be prevented, and to provide an electronic information distribution system therefor. Where he signature generator 22 of the user terminal 20 generates signature information S using its own secret key. The electronic watermark-embedding unit 23 embeds the signature information S, generated by the signature generator 22, in the primary encrypted image data that are transmitted (distributed) by the server terminal 10 (col. 32 line 46 to col.34 line 22). Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Moskowitz and Iwamura, because Iwamura's method of embedding of monitored data by using image data (i.e. watermark) would not only promote security

structure in the system of Moskowitz during receiving data from host computing devices but will also provide identifying data that can be securely and robustly included in a digitized signal in a particular efficient manner such that a server computer system can add such data for each delivery of the digitized signal (Iwamura, abstract, and col.1 line 55 to line 64).

13. With respect to claim 44, Moskowitz disclose a transaction-specific watermark embedded in requested digital content, wherein the digital content is received at a server-side computer (see col. 1, lines 60-64; col. 2, lines 58-67; col. 3, lines 19-23; col. 4, lines 6-17).

Although the system disclosed by Moskowitz shows all the features of the claimed limitation, but Moskowitz does not specifically disclose a server side computer causing the computer to enable tracking the requested signal, and sending watermark signal in response to the request.

In an analogous art, Iwamura, on the other hand discloses computing environment that relates to method and apparatus for providing an electronic watermarking method whereby the illegal activities and the illegal distribution of the original data by a server and a user can be prevented, and to provide an electronic information distribution system therefor. Where he signature generator 22 of the user terminal 20 generates signature information S using its own secret key. The electronic watermark-embedding unit 23 embeds the signature information S, generated by the signature generator 22, in the primary encrypted image data that are transmitted (distributed) by the server terminal 10 (col. 32 line 46 to col.34 line 22). Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Moskowitz and Iwamura, because Iwamura's method of embedding

of monitored data by using image data (i.e. watermark) would not only promote security structure in the system of Moskowitz during receiving data from host computing devices but will also provide identifying data that can be securely and robustly included in a digitized signal in a particular efficient manner such that a server computer system can add such data for each delivery of the digitized signal (Iwamura, abstract, and col.1 line 55 to line 64).

14. With respect to claim 47, Moskowitz disclose transaction-specific watermark embedded in requested digital content, the watermark being generated by one or more processors of a server computer (see abstract) configured to perform acts of signal:
generating transaction identification data identifying a received request, including a pattern in the requested digital content to form a watermarked signal using a predetermined basis signal, wherein the transaction identification data can be derived from the pattern, wherein including is designed to introduce no more than a predetermined maximum level of perceptibility to the requested digital content (col. 2, lines 26-46; col. 3,lines 19-23; col. 6,lines 42-52).

Although the system disclosed by Moskowitz shows all the features of the claimed limitation, but Moskowitz does not specifically disclose a server side computer causing the computer to enable tracking the requested signal, and sending watermark signal in response to the request.

In an analogous art, Iwamura, on the other hand discloses computing environment that relates to method and apparatus for providing an electronic watermarking method whereby the illegal activities and the illegal distribution of the original data by a server and a user can be prevented, and to provide an electronic information distribution system therefor. Where he

signature generator 22 of the user terminal 20 generates signature information S using its own secret key. The electronic watermark-embedding unit 23 embeds the signature information S, generated by the signature generator 22, in the primary encrypted image data that are transmitted (distributed) by the server terminal 10 (col. 32 line 46 to col.34 line 22). Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Moskowitz and Iwamura, because Iwamura's method of embedding of monitored data by using image data (i.e. watermark) would not only promote security structure in the system of Moskowitz during receiving data from host computing devices but will also provide identifying data that can be securely and robustly included in a digitized signal in a particular efficient manner such that a server computer system can add such data for each delivery of the digitized signal (Iwamura, abstract, and col.1 line 55 to line 64).

15. Claim 2 rejected as above in rejecting claim 1, where including comprises: retrieving the basis signal, and including the basis signal in the requested signal to form the watermarked signal in such a manner that the pattern is embedded in the watermarked signal and can be recognized in the watermarked signal (see Moskowitz: col. 1, lines 60-64; col. 2, lines 58-67 to col. 3, lines 1-9).

16. Claim 3 rejected as above in rejecting claim 2, wherein including the basis signal comprises: logically dividing the basis signal into segments, and for each segment of the basis signal, adding the segment of the basis signal to a corresponding segment of the requested signal upon a condition in which a corresponding portion of the pattern has a first logical value (see col.

3, lines 59-67 to col. 4, lines 6-17), and subtracting the segment of the basis signal from the corresponding segment of the requested signal upon a condition in which the corresponding portion of the pattern has a second logical value (see Moskowitz: col. 3, lines 59-67 to col. 4, lines 6-17).

17. Claim 4 rejected as above in rejecting claim 1, further comprising: sending from the server computer the watermarked signal in response to the request for the requested signal (see Moskowitz: col. 3, lines 59-67 to col. 4, lines 6-17).

18. Claim 5 rejected as above in rejecting claim 1, wherein including comprises: selecting watermarked signal fragments representing a first logical value for corresponding portions of the pattern which have the first logical value (see Moskowitz: col. 4, lines 6-17; col. 17, lines 18-44); selecting watermarked signal fragments representing a second logical value for corresponding portions of the pattern which have the second logical value (see Moskowitz: col. 4, lines 6-17; col. 17, lines 18-44); and

combining the watermarked signal fragments representing the first and second logical values to form the watermarked signal (see Moskowitz: col. 4, lines 6-17; col. 17, lines 18-44).

19. Claim 6 rejected as above in rejecting claim 5, wherein the watermarked signal fragments are compressed such that combining the watermarked signal fragments comprise the watermarked signal in a compressed form (Moskowitz: col. 17, lines 18-27).

20. Claim 8 rejected as above in rejecting claim 7, further comprising: for each of the segments of the requested signal (col. 3, lines 50-59): selecting from first and second embedded segments of the composite signal according to a corresponding bit of the transaction-specific identification data (Moskowitz: col. 4, lines 6-17).

21. Claim 9 rejected as above in rejecting claim 8, further comprising: combining the selected embedded segments of the composite signal to form a watermarked signal which includes the transaction-specific identification data embedded therein (see Moskowitz: col. 4, lines 6-17; col. 18, lines 18-44).

22. Claim 10 rejected as above in rejecting claim 7, wherein including both the first and second embedded segments in a composite signal comprises: including the first embedded segment in a first frame, compressing the first frame to form a first compressed frame, including the second embedded segment in a second frame, compressing the second frame to form a second compressed frame, and including both the first and second compressed frames in the composite signal (see Moskowitz: col. lines 6-17; col. 17, lines 18-27).

23. Claim 11 rejected as above in rejecting claim 10, wherein including both the first and second embedded segments in a composite signal further comprises: determining that the first and second compressed frames are equivalent; and including a single compressed frame in the

composite signal to represent both the first and second compressed frames (see Moskowitz: col. 4, lines 6-17; col. 17, lines 18-26; col. 18, lines 1-6).

24. Claim 13 rejected as above in rejecting claim 12, wherein the first and second marked segments are compressed such that watermarked signal formed by combining the selected segments is compressed (see Moskowitz: col. 17,lines 18-27).

25. Claim 15 rejected as above in rejecting claim 14, where including comprises: retrieving the basis signal, and including the basis signal in the requested signal to form the watermarked signal in such a manner that the pattern is embedded in the watermarked signal and can be recognized in the watermarked signal (see Moskowitz: col. 1, lines 60-64; col. 2, lines 58-67 to col. 3, lines 1-9).

26. Claim 16 rejected as above in rejecting claim 15, wherein including the basis signal comprises: logically dividing the basis signal into segments, and for each segment of the basis signal, adding the segment of the basis signal to a corresponding segment of the requested signal upon a condition in which a corresponding portion of the pattern has a first logical value (see Moskowitz: col. 3, lines 59-67; col. 4, lines 6-17); and subtracting the segment of the basis signal from the corresponding segment of the requested signal upon a condition in which the

corresponding portion of the pattern has a second logical value (see Moskowitz: col. 3, lines 59-67; col. 4, lines 6-17).

27. Claim 17 rejected as above in rejecting claim 14, wherein the computer code, when executed by the computer, further causes the computer to enable tracking a requested signal by: sending the watermarked signal in response to the request for the requested signal (see Moskowitz: col. 3, lines 59-67, and col. 4, lines 6-17).

28. Claim 18 rejected as above in rejecting claim 14, wherein including comprises: selecting watermarked signal fragments representing a first logical value for corresponding portions of the pattern which have the first logical value (see Moskowitz: col. 4, lines 6-17; col. 17, lines 18-44); selecting watermarked signal fragments representing a second logical value for corresponding portions of the pattern which have the second logical value (see Moskowitz: col. 4, lines 6-17; col. 17, lines 18-44); and combining the watermarked signal fragments representing the first and second logical values to form the watermarked signal (see Moskowitz: col. 4, lines 6-17; col. 17, lines 1844).

29. Claim 19 rejected as above in rejecting claim 18, wherein the watermarked signal fragments are compressed such that combining the watermarked signals fragments forms the watermarked signal in a compressed form (see Moskowitz: col. 17, lines 18-27).

30. Claim 21 rejected as above in rejecting claim 20, wherein the computer code, when executed by the computer, further causes the computer to enable embedding of transaction-specific identification data into a requested signal by: for each of the segments of the requested signal, selecting from first and second embedded segments of the composite signal according to a corresponding bit of the transaction-specific identification data (see Moskowitz: col. 3, lines 10-22, 59-62; and col. 4, lines 6-17).

31. Claim 22 rejected as above in rejecting claim 21, wherein the computer code, when executed by the computer, further causes the computer to enable embedding of transaction-specific identification data into a requested signal by combining the selected embedded segments of the composite signal to form a watermarked signal which includes the transaction-specific identification data embedded therein (see Moskowitz: col. 4, lines 6-17; col. 10, lines 18-51).

32. Claim 23 rejected as above in rejecting claim 20, wherein including both the first and second embedded segments in a composite signal comprises including the first embedded segment in a first frame, compressing the first frame to form a first compressed frame, including the second embedded segment in a second frame, compressing the second frame to form a second compressed frame, and including both the first and second compressed frames in the composite signal (see Moskowitz: col. 4, lines 6-17; col. 17, lines 18-27).

33. Claim 24 rejected as above in rejecting claim 23, wherein including both the first and second embedded segments in a composite signal further comprises: determining that the first and second compressed frames are equivalent; and including a single compressed frame in the composite signal to represent both the first and second compressed frames (see Moskowitz: col. 4, lines 6-17; col. 17, lines 18-26; col. 18, lines 1-6).

34. Claim 26 rejected as above in rejecting claim 25, wherein the first and second marked segments are compressed such that watermarked signal formed by combining the selected segments is compressed (see Moskowitz: col. 17, lines 18-27).

35. Claim 28 rejected as above in rejecting claim 27, where including comprises: retrieving the basis signal, and including the basis signal in the requested signal to form the watermarked signal in such a manner that the pattern is embedded in the watermarked signal and can be recognized in the watermarked signal (see Moskowitz: col. 1, lines 60-64; col. 2, lines 58-67 to col. 3, lines 1-9).

36. Claim 29 is rejected as above in rejecting claim 28, wherein including the basis signal comprises: logically dividing the basis signal into segments, and for each segment of the basis signal, adding the segment of the basis signal to a corresponding segment of the requested signal upon a condition in which a corresponding portion of the pattern has a first logical value (see Moskowitz: col. 3, lines 59-67 to col. 4, lines 6-17); and subtracting the segment of the basis signal from the corresponding segment of the requested signal upon a condition in which the

corresponding portion of the pattern has a second logical value (see Moskowitz: col. 3, lines 59-67 to col. 4, lines 6-17).

37. Claim 30 rejected as above in rejecting claim 27, wherein the watermarker, when executed, enables tracking of a requested signal by also: sending the watermarked signal in response to the request for the requested signal (see Moskowitz: col. 3, lines 59-67 to col. 4, lines 6-17).

38. Claim 31 rejected as above in rejecting claim 27, wherein including comprises: selecting watermarked signal fragments representing a first logical value for corresponding portions of the pattern which have the first logical value (see Moskowitz: col. 4, lines 6-17; col. 17, lines 18-44); selecting watermarked signal fragments representing a second logical value for corresponding portions of the pattern which have the second logical value (see Moskowitz: col. 4, lines 6-17; col. 17, lines 18-44); and combining the watermarked signal fragments representing the first and second logical values to form the watermarked signal (see Moskowitz: col. 4, lines 6-17; col. 17, lines 1844).

40. Claim 32 rejected as above in rejecting claim 31, wherein the watermarked signal fragments are compressed such that combining the watermarked signals fragments forms the watermarked signal in a compressed form (see Moskowitz: col. 17, lines 18-22).

41. Claim 34 rejected as above in rejecting claim 33, further comprising: for each of the segments of the requested signal, selecting from first and second embedded segments of the composite signal according to a corresponding bit of the transaction-specific identification data (see Moskowitz: col. 3, lines 10-22, 59-62; col. 4, lines 6-17).

42. Claim 35 rejected as above in rejecting claim 34, wherein the blank watermarker, when executed, enables embedding of transaction-specific identification data into a requested signal by also: combining the selected embedded segments of the composite signal to form a watermarked signal which includes the transaction-specific identification data embedded therein (see Moskowitz: col. 4, lines 6-17; col. 10, lines 18-51).

43. Claim 36 rejected as above in rejecting claim 33, wherein including both the first and second embedded segments in a composite signal comprises: including the first embedded segment in a first frame, compressing the first frame to form a first compressed frame, including the second embedded segment in a second frame, compressing the second frame to form a second compressed frame, and including both the first and second compressed frames in the composite signal (see Moskowitz: col. 4, lines 6-17; col. 17, lines 18-27).

44. Claim 37 rejected as above in rejecting claim 36, wherein including both the first and second embedded segments in a composite signal further comprises: determining that the first and second compressed frames are equivalent; and including a single compressed frame in the

composite signal to represent both the first and second compressed frames (see Moskowitz: col. 4, lines 6-17; col. 17, lines 18-26; col. 18, lines 1-6).

45. Claim 39 rejected as above in rejecting claim 38, wherein the first and second marked segments are compressed such that water-marked signal formed by combining the selected segments is compressed (see Moskowitz: col. 17, lines 18-27).

46. Claim 41 rejected as above in rejecting claim 40, wherein two or more segments of the subject signal are represented in a composite frame and further wherein the composite frame includes the following frame instances:

(i) the first segment instance of a first of the two or more segments of the composite frame and the first segment instance of a second of the two or more segment of the composite frame (see Moskowitz: col. 4, lines 1-31; col. 14, lines 26-44);

(ii) the first segment instance of the first segment of the composite frame and the second segment instance of the second segment of the composite frame (see Moskowitz: col. 4, lines 1-31; col. 14, lines 26-44);

(iii) the second segment instance of the first segment of the composite frame and the first segment instance of the second segment of the composite frame (see Moskowitz: col. 4, lines 1-31; col. 14, lines 26-44); and

(iv) the second segment instance of the first segment of the composite frame and the second segment instance of the second segment of the composite frame (see Moskowitz: col. 4, lines 1-31; col. 14, lines 26-44). 47.

47. Claim 42 rejected as above in rejecting claim 41, wherein the frame instances (i) through (iv) are compressed (see Moskowitz: col. 17, lines 18-27).

48. Claim 43 rejected as above in rejecting claim 40, wherein the first and second segment instances or each of the segments are compressed (see Moskowitz: col. 17, lines 18-27).

49. Claim 45 rejected as above in rejecting claim 44 wherein the watermark is embedded in a carrier wave transporting the requested digital content via a network to a party who requested the digital content (Moskowitz: col.6 line 40 to col. 7 line 10).

50. Claim 46 rejected as above in rejecting claim 44 wherein two or more segments of a signal representing the requested digital content are included in a composite frame; and further wherein the composite frame includes:

(i) a first segment instance of a first of the two or more segments of the composite frame and the first segment instance of a second of the two or more segment of the composite frame (see Moskowitz: col. 4, lines 1-31; col. 14, lines 26-44);

(ii) the first segment instance of the first segment of the composite frame and the second segment instance of the second segment of the composite frame (see Moskowitz: col. 4, lines 1-31; col. 14, lines 26-44);

(iii) a second segment instance of the first segment of the composite frame and the first segment instance of the second segment of the composite frame (see Moskowitz: col. 4, lines 1-31; col. 14, lines 26-44); and

(iv) the second segment instance of the first segment of the composite frame and the second segment instance of the second segment of the composite frame (see Moskowitz: col. 4, lines 1-31; col. 14, lines 26-44).

51. Claim 48 rejected as above in rejecting claim 47, wherein the watermark is transporting the requested digital content via a embedded in a carrier wave transporting the requested digital content via a network to a party who requested (Moskowitz: col.6 line 40 to col. 7 line 10).

52. Claim 49 rejected as above in rejecting claim 47, wherein two or more segments of a signal representing the requested digital content are included in a composite frame; and further wherein the composite frame includes

(i) a first segment instance of a first of the two or more segments of the composite frame and a first segment instance of a second of the two or more segment of the composite frame (see Moskowitz: col. 4, lines 1-31; col. 14, lines 26-44);

(ii) the first segment instance of the first segment of the composite frame and a second segment instance of the second segment of the composite frame (see Moskowitz: col. 4, lines 1-31; col. 14, lines 26-44);

(iii) a second segment instance of the first segment of the composite frame and the first segment instance of the second segment of the composite frame (see Moskowitz: col. 4, lines 1-31; col. 14, lines 26-44); and

(iv) the second segment instance of the first segment of the composite frame and the second segment instance of the second segment of the composite frame (see Moskowitz: col. 4, lines 1-31; col. 14, lines 26-44).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SZ
April 23, 2006